THE UNITED STATES DISTRICT COURT
DISTRICT OF UTAH

LAZARO STERN, CELESTE ALLEN, LISA KUCHERRY, PETER SMITH, and SHARON THOMPSON, individually and on behalf of all others similarly situated, Plaintiffs, v. ACADEMY MORTGAGE CORPORATION, Defendant.	**MEMORANDUM DECISION AND ORDER GRANTING [ECF NO. 49] DEFENDANT'S MOTION TO DISMISS** Case No. 2:24-cv-00015-DBB-DAO District Judge David Barlow

Defendant Academy Mortgage Corporation ("Academy") moves to dismiss Plaintiffs' consolidated class action complaint[1] under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6).[2] For the following reasons, the motion is granted.

BACKGROUND

Academy is a mortgage lender that offers a range of consumer mortgage options.[3] Academy collects and stores certain Personally Identifiable Information ("PII"), such as first and last names, dates of birth, and Social Security numbers, of both customers and employees.[4] Academy may also require other sensitive information, including credit scores and credit history, income, and savings to facilitate its mortgage lending business.[5]

[1] Consolidated Class Action Complaint ("Am. Compl."), ECF No. 41, filed July 18, 2024.
[2] Defendant's Motion to Dismiss Plaintiffs' Complaint ("MTD"), ECF No. 49, filed Sep. 9. 2024.
[3] Am. Compl. ¶ 2.
[4] *Id.* at ¶ 89.
[5] *Id.* at ¶ 90.

On or around March 21, 2023, Academy discovered that an unauthorized third party had accessed its computer network (the "Data Breach").[6] The Data Breach gave the third party access to approximately 284,443 individuals' PII.[7] Plaintiffs allege Academy was hacked by ransomware gang BlackCat/Alphv ("BlackCat"), which reportedly took credit for the Data Breach and issued a ransom demand to Academy in May 2023.[8] Plaintiffs believe BlackCat "is anticipated to release all stolen information onto the dark web for access, sale and download following the deadline of the ransom demand."[9] Plaintiffs do not identify when the ransom deadline is.

On December 20, 2023, Academy publicly announced the Data Breach by sending letters notifying customers that it had detected the presence of an unauthorized third party in its network.[10] Plaintiffs Lazaro Stern ("Mr. Stern"),[11] Celeste Allen ("Ms. Allen"),[12] and Lisa Kucherry ("Ms. Kucherry")[13] are former Academy customers who received the notice that their PII was exposed. These plaintiffs have spent time trying to mitigate the risk of identity theft due to the Data Breach.[14] Mr. Stern, Ms. Allen, and Ms. Kucherry allege that they have started receiving text messages related to taking out a line of credit and experienced an increase in spam calls.[15]

---

[6] *Id.* at ¶ 3.
[7] *Id.* at ¶ 102.
[8] *Id.* at ¶¶ 103–106.
[9] *Id.* at ¶ 105.
[10] *Id.* at ¶ 98.
[11] *Id.* at ¶ 22.
[12] *Id.* at ¶ 35.
[13] *Id.* at ¶ 47.
[14] *Id.* at ¶ 29, ¶ 41, ¶ 53.
[15] *Id.* at ¶ 32, ¶ 56.

Plaintiff Peter Smith ("Mr. Smith"), a former Academy customer, claims his identity was stolen after the data breach.[16] Mr. Smith's credit report indicates that a loan was taken out in his name on April 21, 2023, about a month after the Data Breach.[17] Mr. Smith now fears for his personal financial security due to the use of his PII.[18]

Plaintiff Sharon Thompson ("Ms. Thompson") is a former Academy employee whose PII was reportedly exposed during the Data Breach.[19] Ms. Thompson also fears for her personal financial security because of the Data Breach and has experienced a significant increase in spam calls.[20] All named Plaintiffs report feeling anxiety and fear due to the Data Breach.[21]

On January 5, 2024, Plaintiffs filed a complaint on behalf of themselves and a proposed class against Academy, asserting state law claims for negligence,[22] breach of implied contract,[23] unjust enrichment,[24] invasion of privacy,[25] and violations of state Consumer Protection Acts.[26] Plaintiffs seek both monetary and injunctive relief.[27] On June 10, 2024, the court consolidated three related actions.[28] Plaintiffs filed their Amended Complaint on June 18, 2024, and Academy

[16] *Id.* at ¶ 65.
[17] *Id.*
[18] *Id.* at ¶ 67.
[19] *Id.* at ¶ 71–72.
[20] *Id.* at ¶ 79–80.
[21] *Id.* at ¶ 30, ¶ 42, ¶ 54, ¶ 67, ¶ 79.
[22] *Id.* at 52.
[23] *Id.* at 57.
[24] *Id.* at 59.
[25] *Id.* at 60.
[26] *Id.* at 62–63.
[27] *Id.* at 65.
[28] Memorandum Decision and Order Granting Amended Motion to Consolidate Related Cases, ECF No. 40, filed June 18, 2024.

filed its Motion to Dismiss on September 8, 2024.[29] Plaintiffs filed their Memorandum in Opposition on October 7, 2024,[30] and Defendants responded on October 31, 2024.[31]

STANDARD

Standing is "an element of subject matter jurisdiction."[32] The court has a "duty to consider unargued obstacles to subject matter jurisdiction."[33] "The burden of establishing subject matter jurisdiction is on the party asserting jurisdiction."[34] Where standing is challenged at the pleading stage by a Rule 12(b)(1) motion, the court "must presume that the general allegations in the complaint encompass the specific facts necessary to support those allegations."[35] Plaintiffs must plead and ultimately prove the three elements of standing:

> First, the plaintiff must have suffered an injury in fact that is both concrete and particularized and actual or imminent, not conjectural or hypothetical. Second, the plaintiff's injury must be fairly traceable to the challenged action of the defendant, meaning that there must be a causal connection between the injury and the conduct complained of. Third, it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.[36]

---

[29] Defendant's Motion to Dismiss Plaintiffs' Complaint ("MTD"), ECF No. 49, filed Sep. 9. 2024.
[30] Plaintiffs' Memorandum of Law in Opposition to Defendant's Motion to Dismiss ("Opp."), ECF No. 50, filed Oct. 7, 2024.
[31] Reply in Support of Motion to Dismiss ("Reply"), ECF No. 53, filed Oct. 31, 2024.
[32] *Hill v. Vanderbilt Cap. Advisors, LLC*, 702 F.3d 1220, 1224 (10th Cir. 2012) (citations omitted).
[33] *Colorado Outfitters Ass'n v. Hickenlooper*, 823 F.3d 537, 544 (10th Cir. 2016) (quoting *U.S. ex rel. Ramseyer v. Century Healthcare Corp.*, 90 F.3d 1514, 1518 n.2 (10th Cir. 1996)) (emphasis omitted); *see also Image Software, Inc. v. Reynolds & Reynolds Co.*, 459 F.3d 1044, 1048 (10th Cir. 2006) (quoting *Arbaugh v. Y&H Corp.*, 546 U.S. 500, 506 (2006) ("Federal courts 'have an independent obligation to determine whether subject-matter jurisdiction exists, even in the absence of a challenge from any party'").
[34] *Port City Properties v. Union Pac. R. Co.*, 518 F.3d 1186, 1189 (10th Cir. 2008) (citing *Basso v. Utah Power & Light Co.*, 495 F.2d 906, 909 (10th Cir. 1974)).
[35] *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 104 (1998) (citing *Lujan v. Nat'l Wildlife Fed'n*, 497 U.S. 871, 889 (1990)).
[36] *Dep't of Educ. v. Brown*, 600 U.S. 551, 561 (2023) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992)) (cleaned up).

"[A]t the pleading stage, the plaintiff must clearly allege facts demonstrating each element" of standing.[37] "[P]lantiffs must demonstrate standing for each claim that they press and for each form of relief they seek."[38]

DISCUSSION

There are six alleged grounds for standing in the Amended Complaint. All Plaintiffs allege that the Data Breach has harmed them by reducing the value of their PII,[39] that it has cost them time and effort spent trying to mitigate the Breach's impacts,[40] emotional harm,[41] and that the Breach increased the risk of fraud, identity theft, or misuse of their PII.[42] Mr. Stern, Ms. Allen, Ms. Kucherry, and Ms. Thompson also allege that they have started receiving an increase in spam calls since the Data Breach.[43] Finally, Mr. Smith alleges that he was harmed by the Data Breach because a loan was taken out in his name on April 21, 2023.[44]

"To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not merely conjectural or hypothetical.'"[45] "For an injury to be particularized, it must affect the plaintiff in a personal and individual way."[46] Although "[p]articularization is necessary to establish injury in fact," it is not sufficient.[47] An injury must also be concrete; "that is, it must

---

[37] *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016), *as revised* (May 24, 2016) (quoting *Warth v. Seldin*, 422 U.S. 490, 508 (1975)) (cleaned up).
[38] *TransUnion LLC v. Ramirez*, 594 U.S. 413, 431 (2021) (citations omitted).
[39] Am. Compl. ¶28, ¶ 40, ¶ 52, ¶ 64, ¶ 77.
[40] *Id.* at ¶ 29, ¶ 41, ¶ 53, ¶ 66, ¶ 78.
[41] *Id.* at ¶ 30, ¶ 42, ¶ 54, ¶67, ¶ 79.
[42] *Id.* at ¶ 31, ¶ 43, ¶ 55, ¶ 80.
[43] *Id.* at ¶ 32, ¶ 44, ¶ 56, ¶ 81.
[44] *Id.* at ¶ 65.
[45] *Spokeo, Inc. v. Robins*, 578 U.S. 330, 339 (2016), *as revised* (May 24, 2016) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992)).
[46] *Id.* (internal quotations and citations omitted).
[47] *Id.*

actually exist."[48] "Though concreteness may be more easily satisfied for tangible injuries like physical or monetary harms, intangible injuries. . . may nevertheless be concrete for standing purposes."[49] However, any "threatened injury must be certainly impending to constitute injury in fact. . . allegations of possible future injury are not sufficient."[50]

District courts throughout the Tenth Circuit have adopted the three-factor test from *McMorris v. Carlos Lopez & Associates, LLC.*, to determine whether an injury is sufficiently imminent in the data breach context.[51] First, courts consider whether the data breach was intentional.[52] Second, the test requires consideration of whether the data was misused.[53] Some circuits have found standing despite no allegations of misuse,[54] and the Tenth Circuit has not yet spoken on the issue.[55] However, district courts throughout the Tenth Circuit have predicted that the Court of Appeals will require actual misuse of stolen data to find that plaintiffs have standing, and the court applies this standard here.[56] Third, "courts consider whether the nature of

[48] *Id.* (citing Black's Law Dictionary 479 (9th ed. 2009)).
[49] *Lupia v. Medicredit, Inc.*, 8 F.4th 1184, 1191 (10th Cir. 2021) (citing *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340 (2016), *as revised* (May 24, 2016)).
[50] *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013) (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)) (italics and quotation marks omitted).
[51] 995 F.3d 295, 301–02 (2d Cir. 2021). After *TransUnion*, the Second Circuit in *Bohnak v. Marsh & McLennan Companies, Inc.* 79 F.4th 276 (2d Cir. 2023), clarified that *TransUnion* is the touchstone for determining concrete injury, while *McMorris* is the touchstone for determining an "actual or imminent" injury. *Bohnak*, 79 F.4th at 283; *see also Owen-Brooks v. DISH Network Corp.*, No. 1:23-CV-01168-RMR-SBP, 2024 WL 4338133, at *5 (D. Colo. 2024), *report and recommendation adopted*, No. 1:23-CV-01168-RMR-SBP, 2024 WL 4333660 (D. Colo. 2024) (applying three-part test); *Deevers Stoichev v. Wing Fin. Servs., LLC*, No. 22-CV-0550-CVE-JFJ, 2023 WL 6133181, at *5 (N.D. Okla. 2023) (applying test).
[52] *McMorris*, 995 F.3d at 301.
[53] *Id.* at 302.
[54] *Pisciotta v. Old Nat. Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007) (injury-in-fact requirement satisfied by threat of future harm).
[55] *Owen-Brooks v. DISH Network Corp.*, No. 1:23-CV-01168-RMR-SBP, 2024 WL 4338133, at *4 (D. Colo. 2024), *report and recommendation adopted*, No. 1:23-CV-01168-RMR-SBP, 2024 WL 4333660 (D. Colo. 2024) (noting that the "Tenth Circuit has not yet ruled on standing in the data breach context").
[56] *Id.* (collecting cases).

the information accessed through the data breach could subject a plaintiff to a risk of identity theft."[57]

The first and third factors have been adequately alleged in this case. Plaintiffs claim their data was obtained by Blackcat, a group of sophisticated cybercriminals, in a targeted attack, meeting the intentionality factor.[58] Plaintiffs also allege their first and last names, dates of birth, and Social Security numbers were obtained in the Data Breach, which could place them at a risk of identity theft.[59]

As to the second factor, Plaintiffs identify just one instance of actual misuse—the fraudulent loan made using Mr. Smith's identity.[60] Identity theft has been recognized as actual misuse of data that is sufficient to establish an injury in fact.[61] The injury is particularized to Mr. Smith and harmed him in a concrete way.[62] Therefore, this harm must be assessed for traceability.

---

[57] *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 302 (2d Cir. 2021).
[58] *See Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 376 (1st Cir. 2023) (data breach was targeted, as it was result of attack by cybercriminals); *Maser v. Commonspirit Health*, No. 1:23-CV-01073-RM-SBP, 2024 WL 2863579, at *7 (D. Colo. 2024) (no dispute that data breach was targeted after cyberattack).
[59] *See Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 154 (3d Cir. 2022) ("disclosure of social security numbers, birth dates, and names is more likely to create a risk of identity theft or fraud."); *Alonzo v. Refresco Beverages US, Inc.*, No. CV 23-22695 (GC) (JBD), 2024 WL 4349592, at *7 (D.N.J. 2024) (disclosure of sensitive data, "particularly social security numbers, names, and dates of birth" cut in favor of finding Plaintiff had alleged an injury-in-fact); *Owen-Brooks v. DISH Network Corp.*, No. 1:23-CV-01168-RMR-SBP, 2024 WL 4338133, at *7 (D. Colo. Aug. 2024), *report and recommendation adopted*, No. 1:23-CV-01168-RMR-SBP, 2024 WL 4333660 (D. Colo. 2024) (data breach involved financially-sensitive information because hackers had allegedly accessed social security numbers, payment card information, and financial account numbers).
[60] Opp. 5.
[61] *Owen-Brooks v. DISH Network Corp.*, No. 1:23-CV-01168-RMR-SBP, 2024 WL 4338133, at *8 (D. Colo. 2024) (actual unauthorized charges establish actual harm); *Deevers Stoichev v. Wing Fin. Servs., LLC*, No. 22-CV-0550-CVE-JFJ, 2023 WL 6133181, at *4 (N.D. Okla. 2023) ("In the data breach context, actual identity theft and fraud are sufficiently concrete injuries.")
[62] Am. Compl. at ¶¶ 65–68.

To have standing, plaintiffs must establish "a causal connection between the injury and the conduct complained of."[63] "[T]o show that an injury is 'fairly traceable' to the challenged conduct, a plaintiff must allege 'a substantial likelihood that the defendant's conduct caused plaintiff's injury in fact.'"[64] "As part of this showing, a plaintiff must establish that its injury was 'not the result of the independent action of some third party not before this court.'"[65] Plaintiffs cannot establish standing based on a "speculative chain of possibilities."[66]

Mr. Smith's PII was actually misused when his identity was stolen.[67] His credit report shows that someone took out a loan using his identity on April 21, 2023, approximately one month after the Data Breach. However, the identity theft occurred weeks before BlackCat allegedly took credit for the attack and issued a ransom demand to Academy.[68] Mr. Smith does not allege that the PII he provided to Academy was posted to the dark web or otherwise made available to third parties between the Data Breach and the date the fraudulent loan was made.[69]

Academy argues that the alleged misuse of Mr. Smith's data cannot give him or any other class member standing because this misuse is not traceable to the Data Breach.[70] Plaintiffs do not claim that the PII accessed through the Data Breach has been published to the dark web—they only anticipate that it will be published.[71] Plaintiffs provide no other allegation about how the Data Breach caused Mr. Smith's identity to be stolen. They have not alleged that any PII from the

---

[63] *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992).
[64] *Santa Fe All. for Pub. Health & Safety v. City of Santa Fe, New Mexico*, 993 F.3d 802, 814 (10th Cir. 2021) (quoting *Nova Health Sys. v. Gandy*, 416 F.3d 1149, 1156 (10th Cir. 2005)).
[65] *Id.* (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992)).
[66] *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 (2013).
[67] Am. Compl. ¶ 65.
[68] *Id.* at ¶ 103.
[69] *Id.*
[70] Reply 2.
[71] Am. Compl. at ¶ 105.

data breach was published on the dark web or otherwise used to steal Mr. Smith's identity. Therefore, Plaintiffs have not plausibly alleged that Mr. Smith's identity theft was caused by the Data Breach. Without a causal link between the Data Breach and the fraudulent loan, the harm is not traceable to Academy and does not confer standing.[72]

Over a year has passed since the alleged Data Breach and Plaintiffs fail to allege that any of their PII has been put onto or found on the dark web. Plaintiffs allege only one instance of actual misuse, which they did not show was traceable to the Data Breach. Therefore, Plaintiffs have failed to demonstrate Article III standing based on the single alleged actual harm.[73]

Plaintiffs argue that their other alleged harms constitute sufficiently concrete injuries to establish standing.[74] Plaintiffs first argue that they have standing because they "suffer from the substantial risk of identity theft and fraud."[75] This risk has allegedly been exacerbated by their PII "being placed in the hands of unauthorized third parties."[76] But Plaintiffs do not allege that their PII has been published on the dark web or otherwise been made available to third parties that may use it to commit identity theft or fraud. Although Plaintiffs anticipate that their information will be released to the dark web, they do not allege this has actually happened since

[72] *See McCombs v. Delta Grp. Elecs., Inc.*, 676 F. Supp. 3d 1064, 1073–74 (D.N.M. 2023) (unauthorized access of bank account was not fairly traceable to data breach and did not confer standing); *Blood v. Labette Cnty. Med. Ctr.*, No. 522CV04036HLTKGG, 2022 WL 11745549, at *8 (D. Kan. 2022) (allegation that PII was found on dark was lacked plausible connection to data breach).
[73] *McCombs v. Delta Grp. Elecs., Inc.*, 676 F. Supp. 3d 1064, 1074 (D.N.M. 2023) (granting defendant's motion to dismiss where Plaintiff did not allege PII was posted to dark web and over a year had passed since data breach).
[74] Opp. 4.
[75] Opp. 5.
[76] Amend. Compl. ¶¶ 43, 55, 68, 80, 184.

the Data Breach.[77] The risk that Plaintiffs' information will be used is simply too speculative to show they were injured by the Data Breach.[78]

Plaintiffs also claim that the alleged attack by ransomware group Blackcat establishes their standing, citing *Capiau v. Ascendum Machinery, Inc.*[79] for the proposition that the group's involvement provides "an independent basis" for standing.[80] However, in *Capiau* Blackcat "claimed to have published the stolen data. . . on the dark web."[81] Here, Plaintiffs do not allege that Blackcat has actually published their PII or that their PII has otherwise been found on the dark web.[82] Plaintiffs cannot establish standing by alleging an anticipated harm caused by a third party that has not yet occurred and may never occur; therefore, the involvement of Blackcat alone does not establish standing.[83]

Plaintiffs next argue that the risk of future fraud or identity theft confers standing because the Data Breach caused other injuries, including emotional injuries.[84] While allegations of emotional harm may establish injury in fact, these harms must be paired with a sufficient risk of

---

[77] Amend. Compl. ¶ 105.
[78] Plaintiffs cite one post-*TransUnion* case in support of their risk of fraud argument, *Maser v. Commonspirit Health*, No. 1:23-CV-01073-RM-SBP, 2024 WL 2863579, at *9 (D. Colo. 2024). There, the court found the data breach plaintiff did not have standing because there was no risk of future fraud and recommended that the court dismiss plaintiffs' complaint.
[79] *Capiau v. Ascendum Mach., Inc.*, No. 3:24-CV-00142-MOC-SCR, 2024 WL 3747191, at *5 (W.D.N.C. 2024).
[80] Opp. 7.
[81] *Capiau*, 2024 WL 3747191, at *1.
[82] Amend. Compl. ¶ 105.
[83] *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 153 (3d Cir. 2022) (quoting *Clapper*, 568 U.S. at 409–10, 414 n.5) (emphasis omitted) ("While plaintiffs are not required 'to demonstrate that it is literally certain that the harms they identify will come about,' a 'possible future injury'—even one with an 'objectively reasonable likelihood' of occurring—is not sufficient."); *Williams v. Bienville Orthopaedic Specialists, LLC*, No. 1:23CV232-LG-MTP, 2024 WL 3387169, at *8 (S.D. Miss. 2024) (plaintiff whose identity was stolen after data breach did not have standing, as the mere fact that plaintiffs "experienced misuse of their PII or learned that some of their PII had been stolen after the data breach is insufficient to show that the misuse of their PII is fairly traceable" to the breach at issue) (citing *Masterson v. IMA Fin. Grp., Inc.*, No. 223CV02223HLTADM, 2023 WL 8647157, at *4 (D. Kan. 2023)) (data breach plaintiffs whose identities were stolen had not established standing because the "only link between the data breach and the claimed misuse is that the misuse came after the data breach").
[84] Opp. 4.

future harm.[85] And Plaintiffs have not sufficiently alleged a substantial risk of future harm. As previously noted, Plaintiffs do not allege that their PII has actually been posted or found on the dark web—their emotional injuries are based on the fear that it might be posted where criminals could access it and then possibly use it. Such attenuated injuries cannot confer standing.[86]

Plaintiffs next argue that the violation of their privacy rights establishes injury in fact.[87] District courts throughout the Tenth Circuit "have required some allegation that personal information has been viewed or 'exposed in a way that would facilitate easy, imminent access.'"[88] Plaintiffs have not made these required allegations, as they have only alleged that cybercriminals accessed their information and may, at some point, put it on the dark web.[89] They have not alleged that it is currently accessible through the dark web or other means. Therefore, the alleged violation of privacy rights does not establish standing.

Plaintiffs also argue they have been injured because their PII is not as valuable following the data breach.[90] Although some courts have found that "a loss in value of personal information

---

[85] *TransUnion LLC v. Ramirez*, 594 U.S. 413, 437–38 (2021) (plaintiffs failed to establish standing because they did not "present evidence that the class members were independently harmed by their exposure to the risk itself—that is, they suffered some other injury (such as emotional injury) from the mere risk" that their information would be shared).

[86] *See Masterson v. IMA Fin. Grp., Inc.*, No. 223CV02223HLTADM, 2023 WL 8647157, at *7 (D. Kan. 2023) (denying standing based on emotional injuries where "there is no risk of future harm that is certainly impending or substantial."); *Legg v. Leaders Life Ins. Co.*, 574 F. Supp. 3d 985, 994 (W.D. Okla. 2021) (denying standing where plaintiffs alleged they were emotionally harmed by an intentional attack by cybercriminals because "a non-imminent risk of possible future injury following the data breach. . . is not sufficient to confer standing.")

[87] Opp. 7.

[88] *Masterson v. IMA Fin. Grp., Inc.*, No. 223CV02223HLTADM, 2023 WL 8647157, at *7 (D. Kan. 2023) (quoting *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 27–28 (D.D.C. 2014)); *see also C.C. v. Med-Data Inc.*, No. 21-2301-DDC-GEB, 2022 WL 970862, at *10 (D. Kan. 2022) (plaintiffs "loss of privacy, in and of itself, is not a concrete harm that can provide the basis for Article III standing.")

[89] Opp. 7–8; *citing Green-Cooper v. Brinker Int'l, Inc.*, 73 F.4th 883, 889 (11th Cir. 2023), *cert. denied sub nom. Brinker Int'l, Inc. v. Steinmetz*, 144 S. Ct. 1457, 218 L. Ed. 2d 689 (2024) (the allegation that plaintiffs credit card and personal information was posted on the dark web was "critical" to establish standing); *Lupia v. Medicredit, Inc.*, 8 F.4th 1184, 1191 (10th Cir. 2021) (addressing intrusion upon seclusion tort based on FDCPA claims); *Gadelhak v. AT&T Servs., Inc.*, 950 F.3d 458, 461–62 (7th Cir. 2020) (addressing privacy torts under TCPA).

[90] Opp. 9.

supports a finding that a plaintiff has suffered an injury in fact,"[91] district courts throughout the Tenth Circuit have required more than the bare allegation that PII has lost value to establish standing.[92] Some courts have found standing when plaintiffs plausibly allege that they intended to sell their PII themselves and that it is less valuable due to the data breach,[93] but there are no such allegations here.

Plaintiffs allege that PII can be sold,[94] but they do not allege that they have tried to sell their information or that they were offered less for their PII due to the beach. Plaintiffs have not plausibly pled they were injured by the alleged reduction in value to their PII.[95] Plaintiffs cite *Smallman v. MGM Resorts International* for the proposition that the Data Breach devalued their PII "by interfering with their fiscal autonomy."[96] *Smallman* found that the data breach victims there sufficiently alleged details about a market for their PII because their information had been posted for sale on multiple dark web sites.[97] Plaintiffs in that case alleged that their information had been stolen and "posted on the dark web for purchase on at least three separate occasions."[98] But Plaintiffs in the present case have not made any similar allegations. Here, Plaintiffs only

---

[91] *Finesse Express, LLC v. Total Quality Logistics, LLC*, No. 1:20CV235, 2021 WL 1192521, at *3 (S.D. Ohio 2021) (citing *Svenson v. Google Inc.*, No. 13–CV–04080–BLF, 2015 WL 1503429, at *5 (N.D. Cal. 2015)). Plaintiffs cite *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 461 (D. Md. 2020) and *In re Experian Data Breach Litig.*, No. SACV 15-1592 AG (DFMX), 2016 WL 7973595, at *5 (C.D. Cal. 2016) for the proposition that there is a "growing trend" to recognize the reduced value of PII as a basis for standing. These cases, both decided before *TransUnion*, have not been followed in district courts throughout the Tenth Circuit.

[92] *See Masterson v. IMA Fin. Grp., Inc.*, No. 223CV02223HLTADM, 2023 WL 8647157, at *7 (D. Kan. 2023) ("Diminution in the value of Plaintiffs' PII and PHI is not a concrete and particularized injury sufficient to confer standing."); *Blood v. Labette Cnty. Med. Ctr.*, No. 522CV04036HLTKGG, 2022 WL 11745549, at *6 (D. Kan. 2022) ("alleged lost value of PII and PHI lacks a concrete and particularized injury.")

[93] *See Masterson*, 2023 WL 8647157, at *7 (collecting cases).

[94] Am. Compl. ¶ 155.

[95] *Legg v. Leaders Life Ins. Co.*, 574 F. Supp. 3d 985, 994 (W.D. Okla. 2021) (denying standing because Plaintiff "fails to allege that he attempted to sell his personal information and was forced to accept a decreased price.")

[96] 638 F. Supp. 3d 1175, 1191 (D. Nev. 2022).

[97] *Id.* at 1191.

[98] *Id.* at 1185.

anticipate that their information *may* be posted on the dark web. They do not allege that any of their PII has been released to the dark web or posted for sale. In sum, *Smallman* does not support Plaintiffs' standing argument.

Plaintiffs next argue that the time and effort they have spent trying to mitigate the effects of the Data Breach establish an injury in fact.[99] But Plaintiffs "cannot manufacture standing by choosing to make expenditures based on hypothetical harm that is not certainly impending."[100] As discussed above, Plaintiffs' fear about misuse of their PII is not certainly impending harm, as no Plaintiff has alleged that their data is actually available on the dark web or otherwise has been transmitted to others for imminent use. Therefore, any mitigation efforts Plaintiffs have made do not confer standing.

Finally, Mr. Stern, Ms. Allen, Ms. Kucherry, and Ms. Thompson allege they have experienced an increase in spam calls and messages since the data breach. Courts across the Tenth Circuit have "declined to confer standing when considering an increase in spam communications."[101] Spam calls and texts are common, and Plaintiffs' receipt of these communications does not show they were injured by Academy or that the increase is traceable to the Data Breach.

---

[99] Opp. 10.

[100] *See Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 402 (2013); *see also McCombs v. Delta Grp. Elecs., Inc.*, 676 F. Supp. 3d 1064, 1073 (D.N.M. 2023) (efforts monitoring accounts and safeguarding PII do not establish a concrete or imminent threat); *Masterson v. IMA Fin. Grp., Inc.*, No. 223CV02223HLTADM, 2023 WL 8647157, at *6 (D. Kan. 2023) (quoting *Blood v. Labette Cnty. Med. Ctr.*, No. 522CV04036HLTKGG, 2022 WL 11745549, at *6 (D. Kan. 2022)).

[101] *McCombs*, 676 F. Supp. 3d at 1074 (collecting cases); *Legg v. Leaders Life Ins. Co.*, 574 F. Supp. 3d 985, 993 (W.D. Okla. 2021) (increase in phishing emails did not plausibly suggest that any actual misuse of plaintiff's PII had occurred); *Blood v. Labette Cnty. Med. Ctr.*, 2022 WL 11745549, at *6 (D. Kan. 2022) ("alleged inconvenient disruptions (such as spam calls, texts, and emails) do not constitute an injury in fact.") (citing *In re Practicefirst Data Breach Litig.*, No. 1:21-CV-00790(JLS/MJR), 2022 WL 354544, at *5 n.8 (W.D.N.Y. 2022), *report and recommendation adopted*, No. 21CV790JLSMJR, 2022 WL 3045319 (W.D.N.Y. 2022) (collecting cases finding that spam communications do not constitute an injury in fact).

For these reasons, Plaintiffs have failed to allege that they have been actually harmed by the Data Breach in a way that is fairly traceable to Academy. They have not demonstrated standing to pursue damages or injunctive relief. Accordingly, the court does not consider Defendant's additional argument that Plaintiffs failed to state a claim.

ORDER

Academy's Motion to Dismiss is GRANTED and the Amended Complaint is DISMISSED without prejudice.[102]

DATED this 17th day of January, 2025.

BY THE COURT

David Barlow
United States District Judge

[102] ECF No. 49.